CLAIMS

What is claimed is:

1.   A method of automatically identifying anomalous situations during system operations , said method comprising:

    recording actions performed by said system as features in a history file;

    automatically creating a model for each feature only from normal data in said history file;

    performing training by calculating anomaly scores of said features;

    establishing a threshold to evaluate whether features are abnormal;

    automatically identifying abnormal actions of said system based on said anomaly scores and said threshold; and

    periodically repeating said training process.

2.   The method in claim 1, wherein said process of creating a model for each feature comprises:

    establishing relationships that exist between said features for normal system operations;

    selecting a labeled feature from said features;

    mathematically rearranging said relationships from the point of view of said labeled feature to create a solution for said labeled feature, wherein said solution comprises a model for said labeled feature;

    selecting different features as said labeled feature and repeating said process of mathematically rearranging said relationships to produce solutions from the point of view of each remaining feature as models for the remaining features.

3.   The method in claim 2, wherein said solution comprises a mathematical statement of what said labeled feature equals in terms of the relationships between the remaining features.

4.   The method in claim 2, wherein said normal system operations comprise said features in said history file at the time said models are created.

5.   The method in claim 1, wherein said training comprises:

predicting the likelihood that each feature will be normal when one or more of the other features are abnormal, using said model of each of said features;

repeating said predicting using different presumptions about other features being normal and abnormal to produce a trained file of a plurality of anomaly scores for each of said features.

6.   The method in claim 5, wherein said trained file provides an normally score for each of said features for each of a plurality of different possible abnormalities.

7.   The method in claim 5, wherein said process of identifying abnormal actions comprises:

determining values of said features for a given operation of said system;

referring to said trained file to retrieve and anomaly score for each of said features;

comparing said anomaly score for each of said features with said threshold to determine whether each anomaly score exceeds said threshold.

8.   A method of automatically identifying anomalous situations during system operations, said method comprising:

recording actions performed by said system as features in a history file;

automatically creating a model for each feature only from normal data in said history file;

performing training by calculating anomaly scores of said features;

establishing a threshold to evaluate whether features are abnormal;

automatically identifying abnormal actions of said system based on said anomaly scores and said threshold; and

periodically repeating said training process,

wherein said process of creating a model for each feature comprises:

establishing relationships that exist between said features for normal system operations;

selecting a labeled feature from said features;

mathematically rearranging said relationships from the point of view of said labeled feature to create a solution for said labeled feature, wherein said solution comprises a model for said labeled feature;

selecting different features as said labeled feature and repeating said process of mathematically rearranging said relationships to produce solutions from the point of view of each remaining feature as models for the remaining features.

9. The method in claim 8, wherein said solution comprises a mathematical statement of what said labeled feature equals in terms of the relationships between the remaining features.

10. The method in claim 8, wherein said normal system operations comprise said features in said history file at the time said models are created.

11. The method in claim 8, wherein said training comprises:

predicting the likelihood that each feature will be normal when one or more of the other features are abnormal, using said model of each of said features;

repeating said predicting using different presumptions about other features being normal and abnormal to produce a trained file of a plurality of anomaly scores for each of said features.

12. The method in claim 11, wherein said trained file provides an normally score for each of said features for each of a plurality of different possible abnormalities.

13. The method in claim 11, wherein said process of identifying abnormal actions comprises:
determining values of said features for a given operation of said system;
referring to said trained file to retrieve and anomaly score for each of said features;
comparing said anomaly score for each of said features with said threshold to determine whether each anomaly score exceeds said threshold.

14. A method of automatically identifying anomalous situations during system operations, said method comprising:

recording actions performed by said system as features in a history file;

automatically creating a model for each feature only from normal data in said history file;

performing training by calculating anomaly scores of said features;

establishing a threshold to evaluate whether features are abnormal;

automatically identifying abnormal actions of said system based on said anomaly scores and said threshold; and

periodically repeating said training process,

wherein said training comprises:

predicting the likelihood that each feature will be normal when one or more of the other features are abnormal, using said model of each of said features;

repeating said predicting using different presumptions about other features being normal and abnormal to produce a trained file of a plurality of anomaly scores for each of said features.

15. The method in claim 14, wherein said process of creating a model for each feature comprises:

establishing relationships that exist between said features for normal system operations;

selecting a labeled feature from said features;

mathematically rearranging said relationships from the point of view of said labeled feature to create a solution for said labeled feature, wherein said solution comprises a model for said labeled feature;

selecting different features as said labeled feature and repeating said process of mathematically rearranging said relationships to produce solutions from the point of view of each remaining feature as models for the remaining features.

16. The method in claim 15, wherein said solution comprises a mathematical statement of what said labeled feature equals in terms of the relationships between the remaining features.

17. The method in claim 15, wherein said normal system operations comprise said features in said history file at the time said models are created.

18. The method in claim 14, wherein said trained file provides a normally score for each of said features for each of a plurality of different possible abnormalities.

19. The method in claim 14, wherein said process of identifying abnormal actions comprises:
determining values of said features for a given operation of said system;
referring to said trained file to retrieve and anomaly score for each of said features;
comparing said anomaly score for each of said features with said threshold to determine whether each anomaly score exceeds said threshold.

20. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform a method of automatically identifying anomalous situations during system operations, said method comprising:
recording actions performed by said system as features in a history file;
automatically creating a model for each feature only from normal data in said history file;
performing training by calculating anomaly scores of said features;
establishing a threshold to evaluate whether features are abnormal;
automatically identifying abnormal actions of said system based on said anomaly scores and said threshold; and
periodically repeating said training process.

21. The program storage device in claim 20, wherein said method further comprises a process of creating a model for each feature comprises:
establishing relationships that exist between said features for normal system operations;
selecting a labeled feature from said features;
mathematically rearranging said relationships from the point of view of said labeled feature to create a solution for said labeled feature, wherein said solution comprises a model for said labeled feature;

selecting different features as said labeled feature and repeating said process of mathematically rearranging said relationships to produce solutions from the point of view of each remaining feature as models for the remaining features.

22. The program storage device in claim 21, wherein said method further comprises a mathematical statement of what said labeled feature equals in terms of the relationships between the remaining features.

23. The program storage device in claim 21, wherein said normal system operations comprise said features in said history file at the time said models are created.

24. The program storage device in claim 20, wherein said training method further comprises:
predicting the likelihood that each feature will be normal when one or more of the other features are abnormal, using said model of each of said features;
repeating said predicting using different presumptions about other features being normal and abnormal to produce a trained file of a plurality of anomaly scores for each of said features.

25. The program storage device in claim 24, wherein said trained file provides an normally score for each of said features for each of a plurality of different possible abnormalities.

26. The program storage device in claim 24, wherein said process of identifying abnormal actions further comprises:
determining values of said features for a given operation of said system;
referring to said trained file to retrieve and anomaly score for each of said features;
comparing said anomaly score for each of said features with said threshold to determine whether each anomaly score exceeds said threshold.